

ISO/IEC 13888-3:2020 (E)

Information security — Non-repudiation — Part 3: Mechanisms using asymmetric techniques

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols
5	Requirements
6	Trusted third party involvement
7	Digital signatures
8	Use of non-repudiation tokens with and without delivery authorities
9	Evidence produced by the end entities
9.1	General
9.2	Non-repudiation of origin
9.2.1	Non-repudiation of origin token
9.2.2	Mechanism for non-repudiation of origin
9.3	Non-repudiation of delivery
9.3.1	Non-repudiation of delivery token
9.3.2	Mechanism for non-repudiation for delivery
10	Evidence produced by a delivery authority
10.1	General
10.2	Non-repudiation of submission
10.2.1	Non-repudiation of submission token
10.2.2	Mechanism for non-repudiation of submission
10.3	Non-repudiation of transport
10.3.1	Non-repudiation of transport token
10.3.2	Mechanism for non-repudiation of transport
11	Mechanisms to ensure that an NRT was signed before a time t
11.1	General
11.2	Mechanism using a time-stamping service
11.3	Mechanism using a time-marking service

Page count: 13